

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-035092

(43)Date of publication of application : 09.02.2001

(51)Int.Cl.

G11B 20/12
G11B 27/00

(21)Application number : 11-201179

(71)Applicant : HITACHI MAXELL LTD

(22)Date of filing : 15.07.1999

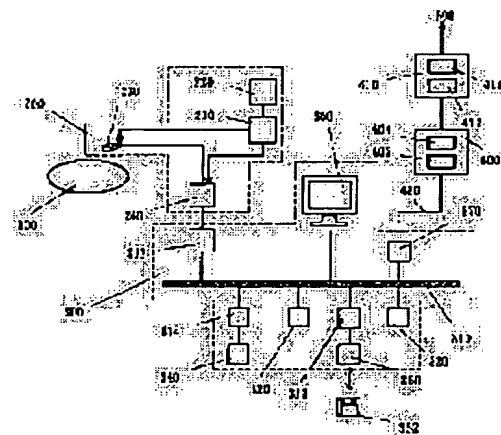
(72)Inventor : SUGA KIMIHARU

(54) REMOVABLE MEMORY, REMOVABLE MEMORY DRIVE AND SECURITY CONTROL METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the security of stored information by setting and controlling the security data by employing the firmware of a removable memory drive of a removable memory.

SOLUTION: Security data are controlled by the firmware of a removable memory drive 200 rather than the OS stored in a hard disk 340 of an external device 300. In other words, the device 300 can not make an access to a removable memory 100 unless a control section 210 discriminates the fact that the security data and a pass word are matched with each other. The possibility of making an access to the memory 100 by the drive 300 is determined without going through the OS of the device 300. Since no professional understands the firmware of the memory 200 unless he is the designer of the drive 200, the security of user's data is improved.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

**Japanese Unexamined Patent Publication
No. 35092/2001 (*Tokukai* 2001-35092)**

A. Relevance of the Above-identified Document

The following is a partial English translation of exemplary portions of non-English language information that may be relevant to the issue of patentability of the claims of the present application.

B. Translation of the Relevant Passages of the Document

See also the attached English Abstract.

[MEANS TO SOLVE THE PROBLEMS]

[0007]

The removal memory ... includes: (i) a management region where management data can be stored but cannot be rewritten by a user; (ii) a data region where data can be recorded or reproduced by the user; and (iii) a security region where security data can be stored. The security data is set and managed by firmware stored in the removal memory of the removal memory drive, so as to control access to the removal memory. With the removal memory drive, the security data is set and managed by the firmware in the removal memory drive, not by an OS stored in an external device connected to the removal memory drive.

[0012]

THIS PAGE BLANK (USPTO)

The removal memory drive ... drives the removal memory and can be connected to an external device. The removal memory includes: (i) the management region where management data can be stored but cannot be rewritten by the user; (ii) the data region where data can be recorded or reproduced by the user; and (iii) the security region where security data can be stored. The removal memory drive includes a head, a signal processing unit, a memory, and a control unit. The head is capable of reproducing information from the removal memory, and the signal processing unit is connected to the head and processes output from the head. The memory stores the firmware which manages the management data and the security data. The control unit allows, when the security data reproduced by the head matches a password entered by the user, the external device to access to the removal memory under the control of the firmware...

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-35092

(P2001-35092A)

(43) 公開日 平成13年2月9日 (2001.2.9)

(51) Int.Cl.

識別記号

FI

テ-マ-ト (参考)

G 1 1 B 20/12
27/00

G 1 1 B 20/12
27/00

5 D 0 4 4
5 D 1 1 0

D

審査請求 未請求 請求項の数10 OL (全 13 頁)

(21) 出願番号 特願平11-201179

(22) 出願日 平成11年7月15日 (1999.7.15)

(71) 出願人 000005810

日立マクセル株式会社

大阪府茨木市丑寅1丁目1番88号

(72) 発明者 菅 君春

大阪府茨木市丑寅一丁目1番88号 日立マ
クセル株式会社内

(74) 代理人 100110412

弁理士 藤元 亮輔

Fターム (参考) 5D044 BC01 CC04 DE02 DE48 DE52

5D110 AA13 DA01 DA12 DB02 DC11

(54) 【発明の名称】 リムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法

(57) 【要約】

【課題】 本発明は、格納された情報の機密性を従来よりも高めることができるリムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法を提供することを例示的目的とする。

【解決手段】 本発明のリムーバブルメモリはドライブのファームウェアによって設定及び管理されるセキュリティ領域を有している。このため、ドライブに接続されているオペレーションシステムではなく、ドライブのファームウェアによってリムーバブルメモリへのアクセスは管理される。

40

| ID部 50 | | | | GAP 60 | データ部 70 | | | | | GAP 60 |
|----------------|-----------------|-----------------|-----------------|-----------|-----------------|------------------|-------------------|------------------|------------------|-----------|
| ID 同期 52 | ID マ-ク 54 | ID データ 56 | ID EDC 58 | | データ 同期 72 | データ マ-ク 74 | データ バ-イト 76 | データ EDC 78 | データ ECC 79 | |

57

(2)

1

【特許請求の範囲】

【請求項1】 管理データを格納可能でユーザが書換え不能な管理領域と、

前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリであって、

前記セキュリティデータは前記リムーバブルメモリへのアクセスを制御するために前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにより設定及び管理されるリムーバブルメモリ。

【請求項2】 前記リムーバブルメモリはディスク状媒体である請求項1記載のリムーバブルメモリ。

【請求項3】 前記セキュリティ領域は前記ユーザがアクセス不能な領域に設けられている請求項1記載のリムーバブルメモリ。

【請求項4】 前記セキュリティ領域は前記リムーバブルメモリに複数点在している請求項1記載のリムーバブルメモリ。

【請求項5】 セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットがユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、

ユーザが入力したセキュリティデータを前記セキュリティ領域に格納する工程とを有し、前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにおいて実行可能なセキュリティフォーマット方法。

【請求項6】 セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットを選択するかどうかをユーザに要求する工程と、前記セキュリティフォーマットが前記ユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、前記ユーザにセキュリティデータを要求する工程と、前記ユーザが入力した前記セキュリティデータを前記セキュリティ領域に格納する工程とを有するユーティリティソフトウェアを格納した情報記録媒体。

【請求項7】 セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットを選択するかどうかをユーザに要求する工程と、前記セキュリティフォーマットが前記ユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、前記ユーザにセキュリティデータを要求する工程と、前記ユーザが入力した前記セキュリティデータを前記セキュリティ領域に格納する工程とを有するユーティリティソフトウェアを通信回線を介して受信する受信部と、前記ユーティリティソフトウェアを配信する送信部とを有する通信システム。

【請求項8】 管理データを格納可能でユーザが書換え

2

不能な管理領域と、

前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記セキュリティ領域をリムーバブルメモリドライブが読み出す工程と、前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、

前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、前記管理領域を読み出して当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、

前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する前記リムーバブルメモリのセキュリティ管理方法。

【請求項9】 管理データを格納可能でユーザが書換え不能な管理領域と、

前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記管理領域をリムーバブルメモリドライブが読み出す工程と、

前記読み出し工程後に前記リムーバブルメモリドライブが前記セキュリティ領域を読み出す工程と、

前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、

前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、

前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する前記リムーバブルメモリのセキュリティ管理方法。

【請求項10】 管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリを駆動すると共に外部装置に接続可能なリムーバブルメモリドライブであって、

前記リムーバブルメモリを再生可能なヘッドと、前記ヘッドに接続されて当該ヘッドの出力を処理する信号処理装置と、

50

(3)

3

前記管理データと前記セキュリティデータとを管理可能なファームウェアを格納したメモリと、前記ファームウェアに従って動作し、前記ヘッドが再生した前記セキュリティデータとユーザが入力したパスワードとが一致する場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする制御装置とを有するリムーバブルメモリドライブ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、一般に情報記録担体及びその駆動装置に係り、特に、ユーザが利用するユーザデータを格納する情報記録担体の前記ユーザデータへのアクセスを制御することを可能にするリムーバブルメモリと当該リムーバブルメモリを駆動するリムーバブルメモリドライブに関する。本発明は、例えば、映像情報、音声情報、テキスト情報、ソフトウェアなどを記録する光ディスク、光磁気ディスク、光サーボ方式を利用したフロッピーディスクなどのディスクにアクセスするためのセキュリティ情報を格納するディスク及びディスクドライブに好適である。また、本発明は、前記ディスク及びディスクドライブを利用したセキュリティ管理方法にも関する。かかるセキュリティ管理方法は、前記セキュリティ情報の生成、格納及び利用方法を含むものである。

【0002】

【従来の技術】一般に、リムーバブルメモリとして、フロッピーディスク（FD）や光磁気（MO）ディスクなどの光ディスクや磁気ディスクなどが知られている。これらのディスクは、一般に、ユーザがアクセスできない管理領域とユーザがアクセス可能なデータ領域とを含んでいる。管理領域は、一般にディスクの制御情報、製造者情報、テスト情報などの管理データを格納しており、データ領域はユーザが利用することができる情報（以下、「ユーザデータ」という。）を格納している。

【0003】従来のディスクは、典型的には、ディスクドライブが接続された外部装置（例えば、パーソナルコンピュータ）のオペレーションシステム（OS）上で管理されており、正当な権限を有しない者にアクセスされたくない情報（機密情報や著作物情報など）をディスクに記録する場合は、OS上からセキュリティをファイルやフォルダ毎にOS上で起動するアプリケーションソフトウェアにより設定して情報へのアクセスを制限していた。アクセス制限は、ユーザデータの漏洩防止だけでなく、ユーザデータの改ざんと消去の防止をも目的にしている。セキュリティの設定及び実行においては、アプリケーションソフトウェアは、典型的に、ディスクドライブのヘッドがディスクから読み取ったデータ、パーソナルコンピュータのキーボードやマウスなどの入力手段を介してユーザが入力したデータ、パーソナルコンピュータのハードディスクに予め格納されているデータ、パー

4

ソナルコンピュータが接続されているモデムなどの通信回線を介して外部の認証機関から送信されるデータ、その他のデータ（例えば、指紋リーダや声紋リーダが読み取るバイオメトリックデータなど）からなるデータの一又は複数のデータを利用して、ユーザが正当な権限を有するものであるかどうかをパーソナルコンピュータの制御部が認証する。

【0004】

【発明が解決しようとする課題】しかし、従来のOSを使用したセキュリティシステムは専門知識を有する者からユーザデータを保護するのに完全とはいえなかった。例えば、OSによるセキュリティ管理はディスクコピーを可能にするため、専門知識を有する者は時間をかけてディスクに記録されたセキュリティデータを解析することができる。また、専門知識を有する者はアプリケーションソフトウェアを解析したり改ざんすることができ、セキュリティを突破することができる。更に、専門知識を有する者はディスクをドライブに挿入してOSを介さずに直接ユーザデータを読み出すことができる。

【0005】

【課題を解決するための手段】そこで、本発明は、このような従来の課題を解決する新規かつ有用なリムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法を提供することを例示的な概括的目的とする。

【0006】より特定的には、本発明は、格納された情報の機密性を従来よりも高めることができるリムーバブルメモリ、リムーバブルメモリドライブ及びセキュリティ管理方法を提供することを例示的目的とする。

【0007】かかる目的を達成するために、本発明の例示的一態様としてのリムーバブルメモリは、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有し、前記セキュリティデータは前記リムーバブルメモリへのアクセスを制御するために前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにより設定及び管理される。かかるリムーバブルメモリによれば、セキュリティデータはリムーバブルメモリドライブに接続された外部装置のOSではなくリムーバブルメモリドライブのファームウェアによって設定及び管理される。

【0008】本発明の例示的一態様としてのセキュリティフォーマット方法は、セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットがユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、ユーザが入力したセキュリティデータを前記セキュリティ領域に格納する工程とを有し、前記リムーバブルメモリのリムーバブルメモリドライブのファームウェアにおいて実行可能であ

5

る。本発明の一側面はこのように従来は存在しなかったセキュリティ領域を物理フォーマットの一態様として形成している。従って、セキュリティフォーマットが施されたリムーバブルメモリはセキュリティフォーマットに対応可能なリムーバブルメモリドライブにおいてのみ駆動可能となる。

【0009】本発明の例示的一態様としての情報記録媒体は、セキュリティ領域をリムーバブルメモリに形成するセキュリティフォーマットを選択するかどうかをユーザに要求する工程と、前記セキュリティフォーマットが前記ユーザにより選択された場合に前記セキュリティ領域が存在することを表示するセキュリティフラグを設定して前記セキュリティ領域に格納する工程と、前記ユーザにセキュリティデータを要求する工程と、前記ユーザが入力した前記セキュリティデータを前記セキュリティ領域に格納する工程とを有するユーティリティソフトウェアを格納している。また、本発明の例示的一態様としての通信システムはかかるユーティリティソフトウェアを、通信回線を介して送受信する送受信部を有する。かかる情報記録媒体及び通信システムは、上述のセキュリティフォーマット方法の作用を有するユーティリティソフトウェアを、媒体及び通信システムとして保護するものである。通信システムは、インターネット、専用回線その他の通信回線を介して不法に配信する一助をなすインターネットプロバイダー、商業サービスプロバイダーその他の通信業者が使用する通信システムをカバーするものである。

【0010】本発明の例示的一態様としてのセキュリティ管理方法は、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記セキュリティ領域をリムーバブルメモリドライブが読み出す工程と、前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、前記管理領域を読み出して当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する。かかるセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードとの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。

【0011】本発明の別の例示的一態様としてのセキュ

(4)

6

リティ管理方法は、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリの前記管理領域をリムーバブルメモリドライブが読み出す工程と、前記読み出し工程後に前記リムーバブルメモリドライブが前記セキュリティ領域を読み出す工程と、前記セキュリティデータとユーザが入力したパスワードとが一致するかどうかを前記リムーバブルメモリドライブが判断する工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが一致すると判断した場合に、当該リムーバブルメモリドライブに接続された外部装置に前記管理データを伝達することによって前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする工程と、前記リムーバブルメモリドライブは、前記セキュリティデータと前記パスワードとが不一致であると判断した場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを不能にする工程とを有する。かかるセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードとの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。

【0012】本発明の例示的一態様としてのリムーバブルメモリドライブは、管理データを格納可能でユーザが書換え不能な管理領域と、前記ユーザによる記録及び再生が可能なデータ領域と、セキュリティデータを格納可能なセキュリティ領域とを有するリムーバブルメモリを駆動すると共に外部装置に接続可能で、前記リムーバブルメモリを再生可能なヘッドと、前記ヘッドに接続されて当該ヘッドの出力を処理する信号処理装置と、前記管理データと前記セキュリティデータとを管理可能なファームウェアを格納したメモリと、前記ファームウェアに従って動作し、前記ヘッドが再生した前記セキュリティデータとユーザが入力したパスワードとが一致する場合に、前記外部装置が前記リムーバブルメモリにアクセスすることを可能にする制御装置とを有する。かかるセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードとの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。

【0013】本発明の更なる目的又はその他の特徴は添付図面を参照して説明される好ましい実施例において明らかにされるであろう。

【0014】

【発明の実施の形態】以下、本発明の例示的一態様としてのリムーバブルメモリ100について図1乃至図3を参照して説明する。リムーバブルメモリ100は、磁気ディスク、光ディスク、光磁気ディスクなどを含むが、本実施例では、光サーボ方式を採用する磁気ディスク

(5)

7

(以下、単に「磁気ディスク」という。)をリムーバブルメモリ100の例として説明する。図1に示すように、磁気ディスク100は、管理領域10a及び10bとその間に存在するデータ領域40とを有している。ここで、図1は本発明の例示的に光サーボ方式を採用する磁気ディスクとして具現化されたリムーバブルメモリ100の平面図である。図1に示すように、ディスク100は、周回方向に整列したトラックを有するデータ領域40とグループ80とを有している。ディスク100は特徴的に光学式トラッキングサーボを採用し、グループ80にレーザー光を照射して、グループ80の有無によって変化する反射光の強弱を検出してトラッキングサーボを行い、例えば、2,490 t p iの光トラック密度を実現している。グループ80の数は、例えば、1666/周、930本/面、デューティ比50%である。

【0015】管理領域10a及び10b(以下、特に断らない限り、参照番号10はこれらを総括するものとする。)の各々は、図2に示すように、それぞれ、2つのディスク・メインテナンス・トラック(DMT)20a及び20b(以下、特に断らない限り、参照番号20はこれらを総括するものとする。)を冗長的に有している。もっとも、本発明は管理領域10aと10bがゼロ又は異なる数のDMT20を有することを妨げるものではない。ここで、図2は、管理領域10の構成を示す概略ブロック図である。DMT20はディスク・マッピング*

8

*グ・トラック又はテーブルと呼ばれる場合もある。本実施例では、4つのDMT20には同一のデータを冗長的に格納されているが、一又は複数のDMT20は異なるデータを格納していてもよい。

【0016】管理領域10はユーザがアクセスできない領域である。「アクセスができない」とは、ユーザが通常のリムーバブルメモリドライブを使用した場合にはアクセスできないことを意味し、例えば、ユーザがドライブを改造したり、製造業者と同様の設備を用いた場合にも常に書換えが不能であるという意味ではないことに留意する必要がある。管理領域10aは、例えば、最初に後述するリムーバブルメモリドライブ200のヘッド230がディスク100をアクセスする領域であり、管理領域10bは、例えば、読み終わりを示すバッファ領域であり、管理領域10aと対峙する最内周又は最外周に設けられている。

【0017】表1に示すように、各DMT20は、一のセキュリティ・テーブル(ST)30と、2つのDMTセグメント22及び24を有している。ここで、表1はDMT20の例示的な構造を示している。DMTセグメント22及び24は管理データを格納し、ST30はセキュリティデータを格納する。また、表1において、ST30はDMT20内で先頭に配置されているが、これに限定されないことはいうまでもない。

【表1】

| | | |
|----------------------|--------------|---------------|
| ST30 512バイト | バイト0 | セキュリティ書込みカウント |
| | バイト1 | セキュリティフラグ |
| | バイト2-34 | セキュリティドライブS/N |
| | バイト3 | パスワードリングス |
| | バイト4 | セキュリティレベル 1 |
| | バイト5 | セキュリティレベル 2 |
| | バイト6 | セキュリティレベル 3 |
| | バイト7 | セキュリティレベル 4 |
| | バイト8 | セキュリティレベル 5 |
| | バイト9 | セキュリティレベル 6 |
| | バイト10 | セキュリティレベル 7 |
| | バイト11 | セキュリティレベル 8 |
| | バイト12 | セキュリティレベル 9 |
| | バイト13-127 | リザーブド |
| | バイト128-164 | セキュリティコード |
| | バイト165 FF | |
| | バイト166-511 | 0 |
| DMTセグメント22 512バイト | バイト0 | USN |
| | バイト1-3 | DSC |
| | バイト4 | RSC |
| | バイト5-127 | F |
| | バイト128-130 | TSAゾーン0 |
| | バイト131-133 | TSAゾーン1 |
| | バイト134-454 | |
| | バイト455-457 | TSAゾーン109 |
| | バイト458-511 | F |
| | バイト512-1021 | 再割当セクタ番号 |
| DMTセグメント24 512バイト | バイト1022-1023 | F |

【0018】管理データは、一般に、ディスク100の制御情報、テスト情報、交替ブロック情報、不良セクタフラグ情報などを含んでいる。表1において、USNは更新通し番号(Update Serial Number)、DSCはデータセクタカウント、RSCは再割当セクタカウント(Reassign Sector Count)、TSAゾーンXはゾーンXにおけるトラックスタートアドレス、RSAは再割当セクタアドレス、L

BAは論理ブロックアドレスを示している。

【0019】セキュリティデータが格納されるST30は広義にはセキュリティ領域に配置されることができ、本実施例ではセキュリティ領域は管理領域10内に設けられている。このように、セキュリティ領域はユーザがアクセスできない領域に設けられることが好ましい。これは、(1)本実施例のリムーバブルメモリ100は書換え可能型であるためにセキュリティ領域が

9

データ領域 40 に設けられれば誤ってユーザデータの書き込みに使用される場合があるのでこれを防止する必要があること、(2) ユーザが通常アクセスする領域ではなければ機密保持専用の領域として機能することが可能であることなどによる。但し、ユーザがアクセスできない領域は管理領域 10 に限定されるものではない。例えば、データ領域 40 内であってもユーザデータの記録再生に使用されない所定の目的用に予約された(リザーブド)領域をセキュリティ領域に割り当てることが可能である。従って、セキュリティ領域は管理領域 10 の一部に限定されるものではない。

【0020】ST30 は、ST30 の書き換え回数であるセキュリティ書き込みカウント、セキュリティ領域の有無を表示するセキュリティフラグ、最後のセキュリティを加えたドライブ 200 の通し番号を表示するセキュリティドライブ S/N を有している。パスワードレングスはセキュリティコードに格納されるべきパスワードの長さを表している。セキュリティコードは 36 バイトを有して単純なアスキーコードを含む任意の暗号方法を利用して書き込まれることができる。165 バイト目でセキュリティデータは終了するが、このバイトに限定されないことはいうまでもない。

【0021】セキュリティ 1 乃至 9 には様々なセキュリティレベルを設定することができる。セキュリティレベル 1 は、例えば、ユーザが入力するパスワードと予めディスクに格納されているパスワードとの比較テスト回数が所定の回数を越えた場合にディスク 100 をドライブ 200 から排出する。セキュリティレベル 2 は、例えば、ユーザによるパスワード入力の失敗回数を定義し、規定回数を越えた場合に DMT 20 を消去する。セキュリティレベル 3 は、例えば、セキュリティを加えたドライブ以外の読み出しを禁止する。その他のセキュリティレベルは更に付加的情報(ユーザ名、会社名、電話番号、バイオメトリックデータ、外部機関の認証コードなど)を要求することができる。

【0022】セキュリティデータは、DMT 20 の数に応じて複数の箇所に物理的な距離を隔てて記録されている。複数の個所に記録される管理データの内容は同一及び/又は相違することができる。同一のセキュリティデータを複数の個所に冗長的に記録することはセキュリティデータの欠陥によるデータの損失を回避して信頼性を高める。例えば、図 2 に示す管理領域 10 a の 2 番目の DMT 20 a に格納されているセキュリティデータは最初の DMT 20 a に格納されているセキュリティデータの冗長であってもよい。特に、ディスク媒体は外周又は内周から錆により侵食されてデータが失われる危険性が高いので、セキュリティデータを冗長的に管理領域 10 a 及び 10 b の両方に記録することが好ましい。

【0023】本実施例においては、セキュリティ領域は、ディスクのフォーマット時にユーザがセキュリティ

(6)

10

フォーマットを選択した結果として形成される。ディスクの構造ではなく物理フォーマットのみを変更するだけであるため、本発明は従来のリムーバブルメモリ 100 を使用することができる。本実施例では、各 DMT 20 の先頭に ST 30 が配置されているが、ST 30 の情報は、ばらばらに分割されて又は一括して DMT セグメント 22 及び 24 の中に一個所に又は複数点在して配置されてもよい。

【0024】相違する内容のセキュリティデータを複数の個所に記録することは全てのセキュリティデータを発見しないと意味のあるセキュリティデータが手に入らないことになるためにデータの信頼性を高める。必要があれば、各セキュリティデータのデータセグメントの結合方法に特徴があってもよい。例えば、管理領域 10 a においては図 2 に示す左から右に 2 つの DMT 20 a 内のセキュリティデータが結合され、管理領域 10 b においては右から左に 2 つの DMT 20 b 内のセキュリティデータが結合されるなどである。選択的に、いずれかのデータセグメントがその他の管理データセグメントの結合方法を定義してよい。

【0025】セキュリティデータはユーザデータへのアクセスを管理するのでユーザデータの機密保持を図る効果を有する。一般に、機密性(安全性)のレベルは、セキュリティデータが存在すること、及び、セキュリティデータの判別の困難性に依存する。機密性のレベルは一般にシステムが複雑であればあるほど高くなるが、複雑なシステムはコスト高を招き、信頼性の低下も招く。信頼性のレベルとコストは一般にシステムが単純であればあるほど高くなる。

【0026】かかる問題を解決するために本実施例のセキュリティデータは基本的にはセキュリティフラグとパスワードのみを必須の構成要素としている。この結果、セキュリティデータの情報量をセキュリティデータの存在自体を発見されないほど少なくすることが可能である。セキュリティデータが発見されなければセキュリティデータは判別されず、また、その情報量が少なくれば単純にすることができる。セキュリティデータの機能を考慮すると、本実施例のセキュリティデータには ISO 標準光磁気ディスクの制御トラックのような従来の管理領域の情報量は不要である。もっとも、本発明はセキュリティデータのデータ量を増やすことを排除するものではない。

【0027】また、本実施例ではセキュリティデータの記録領域をトラックの一部に限定しているのでセキュリティデータの存在を目立たなくするのに効果的である。従って、セキュリティ領域はディスク 100 の全周(周回)に亘る必要がなく、ST 30 を記録するのに必要十分な領域だけ確保すればよい。この結果、リムーバブルメモリ 100 が光ディスクである場合にトラック毎にセキュリティデータの存在を判別しようとして顕微鏡など

(7)

11

で調べる悪意者は本実施例のディスク 100 のトラックの一部のみを見てセキュリティデータは存在しないと判断するか、セキュリティデータの調査をあきらめるかもしれない。

【0028】データ領域 40 はユーザが利用できる領域であり、記録再生可能なディスク 100 はこの領域を使用して映像情報、音声情報、テキスト情報、ソフトウェアその他の情報（ユーザデータ）を記録することができる。図 3 に、データ領域 40 の例示的なセクターフォーマットの概略ブロック図を示す。なお、ディスク 100 が再生されると、ヘッドはセクタを左から右に読んでいくものとする。

【0029】図 3 に示すように、データ領域 40 の各トラックは、ID 部 50 とギャップ 60 とデータ部 70 とを有している。ID 部 50 は物理フォーマット時にのみ形成され、ID 同期部 (ID Sync) 52、ID マーク 54、ID データ 56 及び ID エラー検出コード (EDC) 58 を有している。ID 同期部 52 は、ID マーク 54 を見つけるためのハードウェアのための読み出し用トリガであり、ID マーク 54 は ID 部 50 であることを識別する機能を有する。

【0030】ID データ 56 は対応するセクタの ID（識別情報）を表しており、不良セクターフラグとしての情報を有すると共に、属性設定部 57 を有している。ID データ 56 は、例えば、7 バイトの大きさを有しているが、従来においても 20 ビット程度は使用されていなかった。属性設定部 57 は、かかる未使用部を利用して設けられている。属性設定部 57 は、対応するセクタの属性が読み出し専用（リードオンリ）か書換え可能かを識別する。属性設定部 57 が読み出し専用と識別している場合には、データバイトフィールド 76 のユーザデータが読み出し専用になり、書換えができなくなる。ここで、「書換えができない」とは、ユーザが通常のディスク装置を使用した場合には書換え不能であることを意味し、例えば、ユーザがディスク装置を改造したり、製造業者と同様の設備を用いた場合にも常に書換えが不能であるという意味ではないことに留意する必要がある。また、属性設定部 17 が読み出し専用と識別している場合であっても、読み出し自体を確保するために後述する ECC 79 による誤り訂正は可能なように構成されることが好ましい。属性設定部 57 が書換え可能と識別している場合には、データバイトフィールド 76 のユーザデータは書換え可能にユーザに提供される。

【0031】EDC 78（又はこれに代替する機能的に類似のサイクリック冗長チェック (CRC)）は、ID データ 56 が正しいかどうかを検出するがエラーの訂正はしない。選択的に、ディスク 100 は、ID 同期部 52 の前に、セクタ同期部とセクタマークを更に有してもよい。

【0032】ギャップ (Gap) 60 はセクタ間の緩衝

12

を吸収する一種のバッファとして長さ調整のために挿入され、ID 部 50 とデータ部 70 との間とデータ部 70 とその次の ID 部 50 との間に配置されている。

【0033】データ部 70 は、データ同期部 (Data Sync) 72 と、データマーク 74 と、所定のデータ（ユーザデータ）76 と、データエラー検出コード (EDC) 78 と、データエラー訂正コード (ECC) 79 とを有している。データ同期部 72 は、データマーク 74 を見つけるためのハードウェアのための読み出し用トリガであり、データマーク 74 はデータ部 70 であることを識別する機能を有する。ユーザデータはデータバイトフィールド 76 に格納され、例えば、エンドユーザ以外のメーカーが作成した OS、ソフトウェアプログラム、画像情報、テキスト情報、音楽情報などのユーザが記録再生可能なデータなどの情報を含んでいる。データ EDC 78 は、EDC 58 と同様に、データバイトフィールド 76 のユーザデータが正しいかどうかを検出するがエラーの訂正はしない。ECC 79 は、データバイトフィールド 76 のユーザデータのエラー訂正を行って原データを復元することができる。

【0034】本発明の光サーボ方式の磁気ディスク 100 によれば、一枚のディスクの中に読み出し専用（即ち、ROM として機能する）セクタと書換え可能な（即ち、RAM として機能する）セクタとが混在することになる。また、属性設定部 57 が格納されている ID 部 50 はユーザには書換え不能な領域として構成されている。従って、ユーザはセクタの属性を自由に変更することができず、その結果、読み出し専用に設定されたデータを変更することができない。ここで、「書換え不能」とは、ID 部 50 が、ユーザが通常のディスク装置を使用した場合には書換え不能であることを意味し、例えば、ユーザがディスク装置を改造したり、製造業者と同様の設備を用いた場合にも常に書換えが不能であるという意味ではないことに留意する必要がある。

【0035】以下、リムーバブルメモリ 100 と互換性のある本発明の例示的一態様としてのリムーバブルメモリドライブ 200 の概略的な構成について図 4 を参照して説明する。ここで、図 4 は、リムーバブルメモリドライブ 200 の概略ブロック図である。リムーバブルメモリドライブ 200 は、本実施例ではパーソナルコンピュータとして具現化されている外部装置 300 に接続された磁気ディスクドライブとして構成され、制御部 210 と、メモリ 220 と、ヘッド 230 と、信号処理装置 240 とを有している。その他、ドライブ 200 は、図示しないボタンやキーボードなどの入力手段、液晶ディスプレイなどの表示手段を有することができる。

【0036】制御部 210 は、メモリ 220 に格納されたファームウェアの制御の下、ヘッド 230 及び信号処理装置 240 の動作を制御する。ここで、「ファームウェア」は名称の如何を問わずメモリ 220 に格納されて

13

いるソフトウェアをいう。ファームウェアは、ディスク100のフォーマットを行うユーティリティプログラムと、セキュリティ管理を行うセキュリティプログラムを含んでいる。

【0037】ユーティリティプログラム及びセキュリティプログラムは、ドライブ200の製造業者又は製造業者から委託をうけた業者から供給されるプログラムであり、後述されるリムーバブルメモリ（情報記憶媒体であればよい）352又は通信回線430を介してセットアップ、配信及びアップグレードなどが可能である。本実施例によれば、ユーザは通常フォーマットとセキュリティフォーマットを利用することができる。セキュリティプログラムは、正当な権限を有しないユーザがユーザデータのみならずディスク100にアクセスすることを排除することを目的とするものである。ファームウェアの処理の詳細については後述する。

【0038】ヘッド230は、ディスク100の管理データ、セキュリティデータ及びユーザデータを読み出して、信号処理装置240に送信する。もっとも、後述するように、本実施例のヘッド230は、セキュリティデータがディスク100に存在する場合には、メモリ220に格納されたファームウェアに従って制御部210の制御の下、セキュリティデータ又は管理データを最初に抽出して所定の処理を行った後に外部装置300によるユーザデータへのアクセスを許容するため、管理データ、セキュリティデータ及びユーザデータが同時に信号処理装置240に供給されることはない。信号処理装置240は、外部装置300のSCSIインターフェース312に接続されており、管理データ、セキュリティデータ及びユーザデータを復調して原情報を取り出すことができる。

【0039】外部装置300は、PCIバス310と、SCSIインターフェース312と、IDEバス314と、メインメモリ320と、制御部330と、ハードディスクドライブ340と、リムーバブルメモリドライブ350と、リムーバブルメモリ352と、ディスプレイ360と、通信部370とを有している。なお、リムーバブルメモリ352と100は同一で、リムーバブルメモリドライブ350と200は同一でもよい。

【0040】PCIバス310、SCSIインターフェース312、IDEインターフェース314は当業界で周知であるのでここでは詳しい説明は省略する。メインメモリ320は、例えば、RAMやROMなどを含んでおり、制御部330の動作に必要なプログラムがハードディスク340から一時的にロードされたり図示しないキーボード、マウス、ジョイスティックなどの入力手段からの入力が一時的に格納されたり、システム動作に必要な情報を格納したりする。制御部330は各部の動作を制御し、ハードディスク340はウィンドウズ98などのOSその他各部の動作に必要なプログラム（各種ド

(8)

14

ライバーなど)を格納している。リムーバブルメモリドライブ350とリムーバブルメモリ352は、ユーザデータに関連したした情報の記録再生に使用することができるが、本実施例では、ユーティリティプログラムのセットアップ及びアップグレードに使用される。ディスプレイは、例えば、CRTディスプレイから構成される。

【0041】外部装置300は、更に、モデムなどの通信部370を有している。通信部370は、インターネット、アメリカ・オンラインなどの商業専用回線その他の回線からなる通信回線430を介して、更に外部装置500に接続されている。通信回線430がインターネットであれば、より詳細には、外部装置300は、契約しているインターネットサービスプロバイダー（の通信システム）400と、外部装置500が契約しているインターネットサービスプロバイダー（の通信システム）410を介して、外部装置500と更新することができる。インターネットサービスプロバイダー（の通信システム）400及び410は、周知の受信部402及び412と、送信部404及び414とを有している。

【0042】以下、図5及び図6を参照して、リムーバブルメモリドライブ200のセキュリティ管理について説明する。ここで、図5はリムーバブルメモリドライブ200のセキュリティ管理の一例を説明するフローチャートであり、図6はリムーバブルメモリドライブ200のセキュリティ管理の別の例を説明するフローチャートである。

【0043】図5を参照するに、ディスク100がドライブ200に挿入されると、まず、制御部210はファームウェアに従ってヘッド230にDMT20のST30を読み出すように命令して（ステップ1002）、セキュリティフラグが立っているかどうか（オンかどうか）を判断する。制御部210は、ディスク100が挿入されたかどうかを、ドライブ200に設けられてディスク100の挿入に係合などの機械的手段やLEDなどを利用した光学的手段などにより検出する検出部と交信することによって判断することができる。本実施例では、ディスク100にはセキュリティフラグが立っていると仮定されているが、ドライブ200は後述するセキュリティフォーマットを経たにも拘らずセキュリティフラグがたっていないディスク及び通常フォーマットを経たディスクにも互換性あるように構成することができる。かかる場合、制御部210は、セキュリティフラグが立っていない場合（オフの場合）又はST30が存在しないと判断すると、後述のステップ1008を実行することができる。

【0044】さて、制御部210はセキュリティフラグが立っていると判断すると、「チェック・コンディション (Check Condition)」と呼ばれる処理に移行する。チェック・コンディションはフラグがある場合のドライブ200からのエラーコードである。こ

15

のエラーが発生した場合、ドライブ200はそれ自体で、又は外部装置300と協同して、ユーザにパスワードの入力を要求する(ステップ1004)。ユーザへのパスワード要求はディスプレイ360にその旨を表示するか、ドライブ200に設けられている液晶ディスプレイ、スピーカーその他の出力手段を利用して行うことができる。また、赤ランプや警告音などその旨を直接的に表現しなくてもよい。これにตอบสนองして、ユーザは、ドライブ200に設けられているボタンなどの入力装置又は外部装置300に接続されている図示しない入力手段

(キーボード、マウスなど)を利用してパスワードを入力する。制御部210はセキュリティレベルに応じてパスワードと共に追加データの入力を促してもよい。この際、仮に専門知識を有する悪意者がセキュリティを解除しようとコマンドなどでアクセスしようとしてもモードセンス、モードセクタなどで正確なパスワードを入力できなければ後述するようにディスク100そのものへアクセスすることができなくなる。

【0045】次いで、制御部210は、ST30のセキュリティコードに予め格納されているセキュリティデータとユーザが入力したパスワードが一致するかどうかを判断する(ステップ1006)。なお、「一致」とはパスワードとセキュリティコードが完全に同一であることを要求するものではない。例えば、セキュリティコードは許容されるパスワードの一覧表である場合があるからである。その場合には、その表に挙げられている一のパスワードを入力すればよい。必要があれば、ユーザデータ毎にセキュリティレベルを変更してセキュリティレベルの高いデータには複数のパスワードを要求してもよい。制御部210は、セキュリティデータとパスワードが一致していると判断すれば管理領域10のDMTセグメント22及び24を読み出して管理データを信号処理装置240で再生してから外部装置300にSCSIインターフェース312を介して送信する(ステップ1008)。この結果、外部装置300はディスク100にアクセスしてユーザデータの記録再生を行うことができる。

【0046】一方、制御部210は、不一致と判断すればユーザにパスワードの再入力を促して所定回数以内に一致しなければ、又は、不一致と判断すれば即座に、自動的にディスク100をイジェクトする(ステップ1010)。より詳細には、ヘッド230がセキュリティデータをうまく読み取れなかった場合、読み取ったセキュリティデータが理解不能の場合、そしてユーザが入力したパスワードが正しくない場合にはエラー処理が行われる。エラー処理の場合にはディスプレイ360にその旨表示されて再試行などが促されるがいずれにしてもエラー処理においては信号処理装置340はユーザデータを再生することができない。これにより、ユーザデータの外部への流出を防止することができる。

(9)

16

【0047】エラーが確定すれば制御部210はディスク100をイジェクトする。所定回数のパスワードの入力が失敗したディスク100は再度ドライブ200に入力されても制御部210は直ちにエラーを確定してイジェクトすることができる。この結果、外部装置300にはディスク100に関して何の情報もドライブ200から送信されなくなるので、制御部330はディスク100が存在することすら認識できなくなる。

【0048】代替的に、図6に示すように、管理領域を先に読み出して(ステップ1012)、その後ステップ1002から1004を行ってもよい。その後、制御部210は一致と判断すれば既に読み出した管理データを信号処理装置240で再生してから外部装置300にSCSIインターフェース312を介して送信する(ステップ1014)。この結果、外部装置300はディスク100にアクセスしてユーザデータの記録再生を行うことができる。ステップ1012及び1014を採用する場合には、読み出した管理データはメモリ220その他の記憶部に一時的に格納することになるであろう。

【0049】本発明の例示的一態様としてのセキュリティ管理方法によれば、セキュリティデータは外部装置300のハードディスク340に格納されたOSではなくドライブ200のファームウェアによって管理される。即ち、制御部210がセキュリティデータとパスワードの一致があると判断しない限り外部装置300はリムーバブルメモリ100にアクセスすることができない。外部装置300のリムーバブルメモリ100へのアクセス可能性は、外部装置300のOSを介在しないで判断している。リムーバブルメモリドライブ200のファームウェアはドライブ200の設計者でなければ専門知識を有する者であっても理解することができないためにユーザデータの機密性を従来のOSによるセキュリティ管理方式よりも高めることができる。

【0050】次に、図7を参照して、本発明の例示的一態様としてのフォーマット方法を説明する。ここで、図7は、リムーバブルメモリドライブ200が実行するフォーマット方法を示すフローチャートである。まず、ユーザはドライブ200にフォーマットされていない又は既にフォーマットされているディスク100を挿入する。これにตอบสนองして、制御部210は、フォーマット形式の選択をユーザにステップ1004などと同様に促す(ステップ1102)。

【0051】なお、既にフォーマットがなされているディスクが挿入された場合、ユーザはドライブ200に設けられているボタンなどの入力装置又は外部装置300に接続されている図示しない入力手段(キーボード、マウスなど)を利用してフォーマット処理を選択する。既に通常のOS(例えば、ウィンドウズ98)に準拠してフォーマットされていれば、後述するステップ1104ではユーザはセキュリティフォーマットを希望すること

(10)

17

になるであろう。また、既にセキュリティフォーマットがなされていれば、後述するステップ1104ではユーザは通常のフォーマットを希望することになるであろう。セキュリティフォーマットが既にされていれば、ユーザは図5又は図6に示す処理を実行してパスワードその他の情報を入力することによって、外部装置300によるリムーバブルメモリ100へのアクセスを確保しておく必要がある。フォーマット形式を変更する場合には通常はユーザデータの消去を伴う。例えば、EEなどの意味のないデータに変換することによって通常のノンセキュリティディスクとして使用することができる。しかし、代替的に、ユーザデータを消去しないでDMT20のみを変更することができるであろう。

【0052】次に、制御部210は、ユーザが入力したフォーマット形式が通常のフォーマットかセキュリティフォーマットかを判断する(ステップ1104)。ここで、「セキュリティフォーマット」とは、図3に示すST30を形成する物理フォーマットをいう。ユーザが(クイックフォーマットを含む)通常のフォーマットを選択すれば(ステップ1104)、既知のフォーマット方法により管理領域とデータ領域が設定され、管理領域にはST30を含まないDMTが形成される(ステップ1106)。

【0053】一方、ユーザがセキュリティフォーマットを選択すれば(ステップ1104)、制御部210は、管理領域10とデータ領域40が設定され、管理領域10にはST30を含むDMT20が形成されることになる(ステップ1108)。この結果、ディスク100は論理セキュリティディスクになる。なお、上述したように、ST30はデータ領域40に形成されても良いことに留意する必要がある。次に、制御部210はセキュリティフラグを立てる(ステップ1110)。より詳細には、セキュリティフォーマットが選択されてもユーザがパスワードを後述するステップ1112で入力しない場合には実質的に通常のフォーマットと同様であるとみなしてセキュリティフラグを立てないことも可能である。ユーザがパスワードを入力しなかったことはパスワードレングスにより判断することができる。代替的に、いかなる場合にもセキュリティフォーマットにおいてはパスワードを要求してセキュリティフラグを立ててもよい。

【0054】次に、制御部210は、ユーザにパスワードその他に必要なオプションデータの入力(例えば、セキュリティレベルの設定、暗号の必要性、使用される暗号の種類、バイオメトリックデータの必要性、その他の付加的データ(ユーザ名、会社名、電話番号など)の必要性、外部認証機関からの認証の必要性)を促して、入力があるとこれを格納する(ステップ1112)。例えば、周知の暗号プロトコルをセキュリティデータに関与させることができる。例えば、リムーバブルメモリドライブに格納されるデータをオンライン(インターネット

18

や商業オンライン回線など)により送信し、デジタル署名とパブリック/プライベートキーを使用するなどである。

【0055】このようにセキュリティフォーマットが施されたリムーバブルメモリ100はセキュリティフォーマットに対応可能な専用のリムーバブルメモリドライブ200においてのみ駆動可能となる。従って、仮にリムーバブルメモリ100が盗まれても窃取者は専用のリムーバブルメモリドライブ200を有していなければそれに格納されたデータを得ることができないため、ユーザデータの機密性は向上している。

【0056】かかるセキュリティフォーマット方法はユーティリティソフトウェアとして、媒体(例えば、リムーバブルメモリ352)を介して、又は、通信システム400及び410を介して、メモリ220のファームウェアにセットアップ及びアップグレードすることができる。

【0057】図7には記載されていないが、ユーザは一旦設定したパスワードを変更することができる。また、パスワードを忘れてしまった場合に、所定の条件の下以前に入力されたパスワードを無効にすることも可能である。

【0058】ドライブ200は、ディスク100の再生のみでなく記録も行うことができる。上述したように、ディスク100は書換可能型であるためにユーザは以前のユーザデータに所望のデータを付加することができる。ディスク100及びドライブ200は、記録の際には、選択的に、追加的情報の入力と照合を行って再生時よりも機密性を高めてもよい。これにより、例えば、情報の一部が誤った情報に書き換えられたディスク100が頒布されることを防止することができる。アクセスが許可・認証されたユーザにのみがユーザデータに記録をすることができるので以前に記録されたユーザデータが無防備に変更されることは防止される。リムーバブルメモリ100は、例えば、病院の各患者毎の電子カルテ、保険会社の被保険者データ、企業の営業活動データ、公的機関の管理台帳などに使用することができる。

【0059】以上、本発明の好ましい実施例を説明したが、本発明はこれらに限定されずその要旨の範囲内で種々の変形及び変更が可能である。例えば、本発明は、ディスクの種類(CD、光磁気ディスク、DVDなど)は問わない。

【0060】

【発明の効果】本発明の例示的一態様としてのリムーバブルメモリによれば、リムーバブルメモリドライブのファームウェアはリムーバブルメモリドライブの設計者でなければ専門知識を有する者であっても理解することができないためにデータ領域に格納されたユーザデータの機密性を従来のOSによるセキュリティ管理方式よりも高めることができる。

(11)

19

【0061】本発明の例示的一態様としてのセキュリティフォーマット方法によれば、セキュリティフォーマットが施されたリムーバブルメモリはセキュリティフォーマットに対応可能な専用のリムーバブルメモリドライブにおいてのみ駆動可能となる。従って、仮にリムーバブルメモリが盗まれても窃取者は専用のリムーバブルメモリドライブを有していなければそれに格納されたデータを得ることができないため、従来よりも格納されたデータの機密性は向上している。かかるセキュリティフォーマット方法はユーティリティソフトウェアとして、それを格納する媒体とそれを配信する通信システムを本出願において保護するものである。

【0062】本発明の例示的一態様としてのセキュリティ管理方法によれば、リムーバブルメモリドライブによりセキュリティデータとパスワードの一致があると判断されない限り外部装置はリムーバブルメモリにアクセスすることができない。アクセス可能性を外部装置のOSを介在しないで判断しているために、上述のリムーバブルメモリと同様に、従来よりも格納されたデータの機密性は向上している。

【図面の簡単な説明】

【図1】 光サーボ方式を採用する磁気ディスクとして例示的に具現化された本発明の例示的一態様としてのリムーバブルメモリの平面図である。

【図2】 図1に示す磁気ディスクの管理領域の構成を示す概略ブロック図である。

【図3】 図1に示す磁気ディスクのデータ領域のセクタフォーマットを示す概略ブロック図である。

【図4】 図1に示すリムーバブルメモリと互換性のあるリムーバブルメモリドライブの概略ブロック図である。

【図5】 図4に示すリムーバブルメモリドライブが実行可能なセキュリティ管理の一例を説明するフローチャートである。

20

ートである。

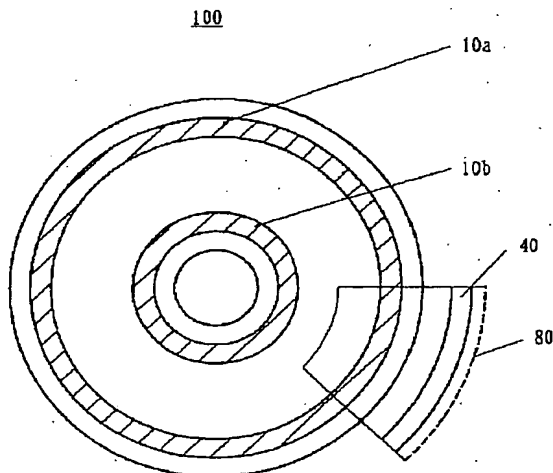
【図6】 図4に示すリムーバブルメモリドライブが実行可能なセキュリティ管理の別の例を説明するフローチャートである。

【図7】 図4に示すリムーバブルメモリドライブが実行するフォーマット方法を示すフローチャートである。

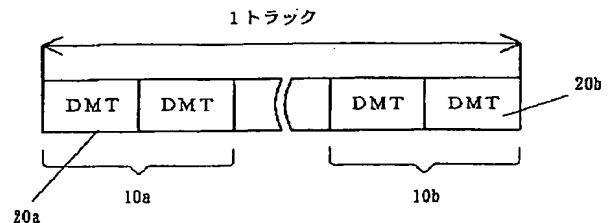
【符号の説明】

| | |
|-----|-------------------|
| 100 | リムーバブルメモリ |
| 10a | 管理領域 |
| 10b | 管理領域 |
| 20a | DMT |
| 20b | DMT |
| 30 | セキュリティ・テーブル |
| 40 | データ領域 |
| 50 | ID部 |
| 60 | ギャップ |
| 70 | データ部 |
| 200 | リムーバブルメモリドライブ |
| 210 | 制御部 |
| 220 | メモリ |
| 230 | ヘッド |
| 240 | 信号処理装置 |
| 300 | 外部装置 |
| 330 | 制御部 |
| 340 | ハードディスク（ドライブ） |
| 350 | リムーバブルメモリドライブ |
| 352 | リムーバブルメモリ（情報記憶媒体） |
| 370 | 通信部 |
| 400 | 通信システム |
| 410 | 通信システム |
| 430 | 通信回線 |

【図1】

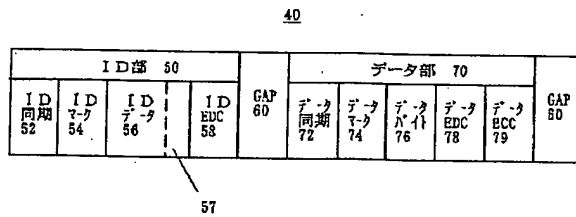


【図2】

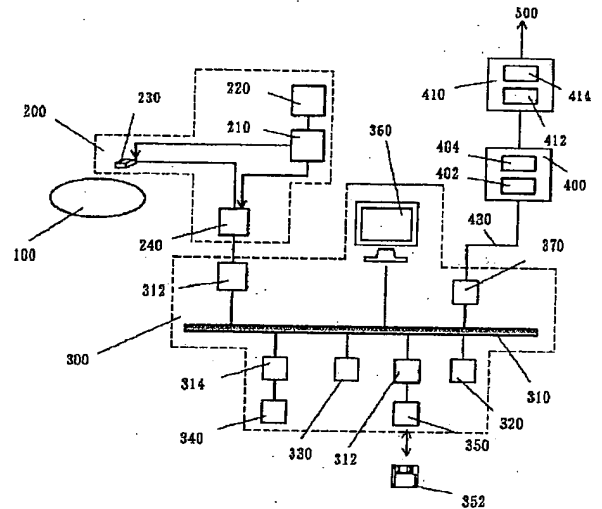


(12)

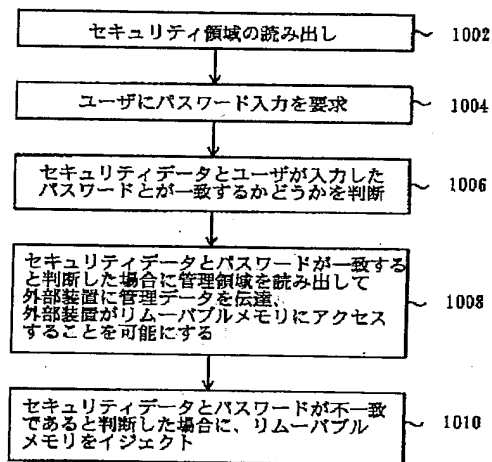
【図 3】



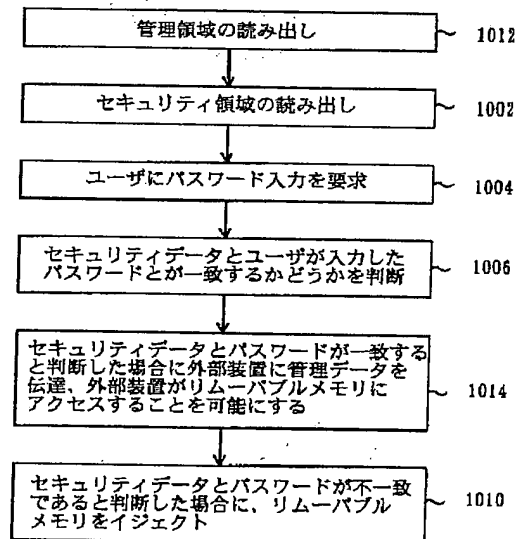
【図 4】



【図 5】

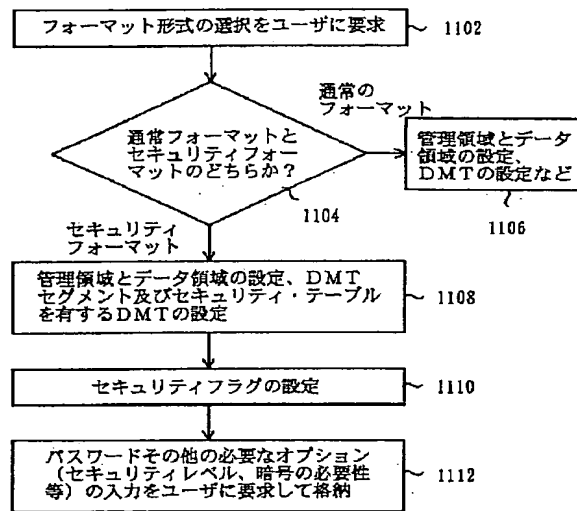


【図 6】



(13)

【図7】



THIS PAGE BLANK (USPTO)